Remarks
Cybersecurity Threats: Safety and Security above Borders
Ambassador Stephen D. Mull
October 28, 2013

Thank you, Mr. Orliński, for your kind introduction. I thank Boeing and the Warsaw Exhibition Board for inviting me to join you. I am pleased to see today many representatives from companies operating critical infrastructure, along with prominent government officials.

Ensuring the integrity of our critical networks remains a primary concern for businesses and governments throughout the world. Despite the greater attention paid to cybersecurity in recent years, there is clearly more we can do to protect our most important computer networks, both in the U.S. and Poland.
In the next few minutes, I will describe a few prominent cyber-attacks, the lessons we learned from them, and some of the mechanisms the U.S. put in place to prevent and mitigate such attacks. These mechanisms call for robust collaboration and information sharing among private and public sector partners. Such team work, even among business competitors, has proven to be highly effective in reducing our vulnerability to cyber threats.

Cyber-Attack Examples

My first example of recent cyber-attacks deals with the financial sector. Financial institutions in all countries are under constant threat of cyber-attacks. In recent months, three major banks in the United States have experienced some of the most advanced and persistent cyber-attacks seen to date, resulting in millions of dollars in losses. U.S. and Polish banks are common targets for distributed denial of service attacks which aim to overwhelm web-based applications and shutdown services. However, in these recent instances the denial of service attacks were serving as a diversion, allowing fraudsters to exploit other weaknesses in the banks' networks to gain access to their wire payment applications. As a result, these intruders sent millions of dollars in fraudulent wire transfers overseas while network security officials were busy addressing the denial of service attacks. This example illustrates the ever-changing nature of the cyber threat and how we must adapt to the evolving tactics of cyber criminals.

As a second example, a little more than a year ago, in Saudi Arabia, the oil giant Saudi Aramco was the victim of one of the most severe cyber-attacks the business world has ever seen. Malicious actors claiming that Saudi Arabia had been responsible for "crimes and atrocities" in countries including Syria and Bahrain gained access to Aramco’s internal network. These individuals leveraged this access to damage over 30,000 of the company’s computers. Aramco stated publicly that as a result of this attack the hardware on 85% of its devices was wiped clean. While the attack failed to stop oil and gas production in Saudi Arabia, it was incredibly damaging to the company’s business and credibility. Just imagine the business consequences of a cyber-incident at one of your firms in which 85% of your computers were completely erased.

Perhaps the most disturbing attack of all in most recent years took place in Estonia in 2007. An organized team launched a missive distributed denial of services attack against the Estonian government, media, telecommunications, and banking websites. The attackers were able to hijack over one million computers in 175 different countries and use them to tie up Estonian internet services for two weeks. During this time Estonian residents could not carrying out basic daily tasks that we take for granted in the 21st century, such as making telephone calls, accessing bank accounts, or paying for groceries with debit cards. The 2007 attack on Estonia served as a “wake-up call” regarding the potential of cyber crimes to impact an entire nation’s critical communications infrastructure.

These three examples are vastly different: the attackers had different motivations and used dissimilar methods. However, the end result is same: millions of dollars in losses and damage to the credibility of these institutions; indeed a serious threat to the national security of a member of NATO. Furthermore, had these attacks fully achieved their objectives, they could have disrupted our worldwide financial system and energy supplies. With these examples in mind, I want to speak about some of the ways we seek to mitigate cyber threats and manage cyber incidents in the United States.

Decision-Making Authority

The need to react quickly is one of the most important lessons learned from these examples of cyber attacks. Managers of critical infrastructure have a short window of opportunity to recognize cyber attacks and take action to mitigate the damage. One way to facilitate such rapid response is for government agencies and private business is to designate the *lowest* level of authority possible to make decisions that could block the spread of an attack. In the Estonian example, the 39-year old head of the Estonian Computer Emergency Response Team took it upon himself to block all incoming foreign traffic to Estonian networks, thereby buying time for his colleagues to neutralize infected computers.

Information Sharing

The cyber attacks I described earlier underscore the need for information sharing among public and private sector operators of critical infrastructure. Unfortunately, transparent communication on cyber crimes is not easy to achieve. For example, the initial response to the cyber attack in Estonia was inhibited by government prohibitions on sharing classified. This is an ongoing problem in every country. Likewise, private businesses, such as U.S. banks that were recently attacked, worry about losing market share if they publicly acknowledge that they have been a victim of cyber crime. Even sharing security success stories is problematic because such information could be used by cyber criminals to counter our defenses.

In the U.S. we have established structures that are designed to overcome these communication barriers. One such structure, so-called “fusion centers,” brings private operators of critical infrastructure together with law enforcement entities. This allows the government to share information on threats with industry quickly, in ways that were previously hampered by bureaucratic processes. The information also flows back to the government, as industry is often better informed than the government on emerging threats. Additionally, in such centers, legal agreements have been reached which allow for competitors in the same market sector to share information on common threats. This trust is not instantly created, but by working together over time and sharing information on common threats, these competitors can mutually prosper and address vulnerabilities before they are exploited. We have found these centers to be some of the most effective tools in promoting transparent information sharing on cyber threats.

Cybersecurity Frameworks

The attack on Saudi Aramco is a reminder that individual private companies need to prepare themselves -- from both a staffing and technology standpoint — to recognize and mitigate cyber attacks quickly. Governments can and ought to play a role in helping companies protect critical infrastructure from cyber attacks. An initiative currently underway in the U.S. is the federal government's efforts to define a voluntary cybersecurity framework for operators of our critical infrastructure. Industry standards will define best practices for securing the computer systems that control our critical infrastructure and assist operators with risk management planning. This effort has been done in close cooperation with the private sector so as to ensure that standards are applicable, relevant, and do not overly burden industry. We expect the draft framework to be completed by February of next year. Such efforts are never really complete though, and our efforts to counter cyber threats will be as persistent as the attackers themselves.

Conclusion

In sum, it is the collective responsibility of businesses and governments to protect cyberspace. This is a worldwide problem, so our cooperation must extend across national borders. The threats facing U.S. networks, especially as related to cybercrime, are much the same as those in Poland. This is why we must increase our cooperation, both government to government and business to business. We must define common practices, continue to develop and adhere to international conventions, and ensure that information can flow freely and in a timely fashion. Collaboration mechanisms, such as the public-private partnerships and industry-specific collaboration centers I described earlier, should be established to help industry and government rapidly and effectively respond to emerging threats. The United States is eager to share our expertise and partner with Poland to address cyber threats. As cyber attacks take on an even greater international character, such partnerships will be absolutely crucial.

Thank you for your time.